Draft

U.S. Department of Defense

Virtual Private Network (VPN) Boundary Gateway

Protection Profile

for

Basic Robustness Environments

Version 0.6

September 10, 2001

Protection Profile Title:

U.S. Department of Defense Virtual Private Network (VPN) Protection Profile for Basic Robustness Environments.

Criteria Version:

This Protection Profile (PP) was developed using Version 2.1 of the Common Criteria (CC) [1].

Constraints:

Targets of Evaluation (TOEs) developed to satisfy this Protection Profile shall conform to CC Part 2 and CC Part 3.

Authors:

This Protection Profile was prepared by:

Linda M. Gilmore, SPARTA, Inc.

Barbara Mayer, SPARTA, Inc.

Howard Weiss, SPARTA, Inc.

Charles Hall, National Security Agency

Acknowledgements:

The authors would like to acknowledge Mike Sheridan, Ronald D. Varnum from the National Security Agency and Eliot Sohmer from ACS Defense, Inc.

Table of Contents

List of Tables

List of Figures

1 PROTECTION PROFILE (PP) INTRODUCTION

1 This Virtual Private Network (VPN) Boundary Gateway Protection Profile (PP) for Basic Robustness Environments was generated under the Enclave Boundary Security Technologies and Solutions (EBST&S) Support Program, sponsored by the National Security Agency (NSA). This PP is intended to be used as follows:

- For product vendors and security product evaluators, this PP defines the requirements that must be addressed by specific products as documented in vendor Security Targets (STs).

- For system integrators, this PP is useful in identifying areas that need to be addressed to provide secure system solutions. By matching the PP with available STs, security gaps may be identified and products or procedures may be configured to bridge these gaps.

1.1 PP IDENTIFICATION

2 **Title:** U. S. Department of Defense Virtual Private Network (VPN) Boundary Gateway Protection Profile (PP) for Basic Robustness Environments

3 **Sponsor:** National Security Agency (NSA)

4 **Authors:** Linda M. Gilmore, Charles Hall, Barbara Mayer, and Howard Weiss

5 **Contributors:** Mike Sheridan, Eliot Sohmer, Ronald D. Varnum

6 **CC Version:** Common Criteria (CC) Version 2.1

7 **Registration:** <to be provided upon registration>

8 **PP Version:** Version 0.6, dated September 10, 2001

9 **Keywords:** Virtual Private Network, VPN, protection profile, Gateway Boundary, encryption, decryption, IPSEC ESP, IKE

1.2 PP OVERVIEW

10 This PP specifies the minimum security requirements for VPN Boundary Gateways (hereafter referred to as the Target of Evaluation (TOE)) used by the Department of Defense (DoD) in basic robustness environments. The target robustness level of "basic" is specified in the *Guidance and Policy for the Department of Defense Global Information Grid Information Assurance (GIG)* [2].

11 The TOE provides the capability for enclaves of systems to communicate sensitive unclassified information securely with other TOE-equipped enclaves. Additionally, enclaves may communicate non-securely with non-VPN-protected sites across an unprotected network infrastructure. The TOE only provides protection of data in transit over a network. It does not provide security for data stored on enclave systems.

12 The TOE has the capability of encrypting network traffic between peer TOEs that enforce the same security policies, authenticating an Authorized Administrator, and auditing security-relevant events that occur on the TOE. TOEs compliant with this PP are intended for use in environments that are restricted to the processing of, up to and including, sensitive unclassified information.

13 This PP defines:

- assumptions about the security aspects of the environment in which the TOE will be used;
- threats that are to be addressed by the TOE;
- security objectives of the TOE and its environment;
- functional and assurance requirements to meet those security objectives; and
- rationale demonstrating how the requirements meet the security objectives.

1.3 CONVENTIONS

14 The notation, formatting, and conventions used in this Protection Profile are largely consistent with those used in version 2.1 of the Common Criteria (CC). Selected presentation choices are discussed here to aid the Protection Profile user.

15 The CC allows several operations to be performed on functional requirements; *refinement*, *selection*, *assignment*, and *iteration* are defined in paragraph 2.1.4 of Part 2 of the CC. Each of these operations is used in this Protection Profile.

The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text**.

The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections are denoted by *underlined italicized text*.

The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignment is indicated by showing the value in square brackets, [assignment_value].

The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing the iteration number in parenthesis following the component identifier, (iteration_number).

The **security target writer** operation is used to denote points in which the final determination of attributes is left to the security target writer. Security target writer operations are indicated by the words {determined by the security target writers} in braces.

16 Application Notes are provided to help the developer, either to clarify the intent of a requirement, identify implementation choices, or to define "pass-fail" criteria for a requirement. For those components where Application Notes are appropriate, the Application Notes will follow the requirement component.

1.4 TERMINOLOGY

17 In the Common Criteria, many terms are defined in Section 2.3 of Part 1. The following are a subset of those definitions. They are listed here to aid the user of this Protection Profile.

Authorized Administrator -- A role which human users may be associated with to administer the security parameters of the TOE. An Authorized Administrator is not subject to any access control requirements once authenticated to the TOE and is therefore trusted to not compromise the security policy enforced by the TOE. Authorized Administrators may administer the TOE remotely over a network connection, via a directly connected console, or via a local area network. All of the discussions and requirements in the PP apply to all three means of access. This role may be assumed by a security/system administrator.

External IT entity -- Any Information Technology (IT) product or system outside of the TOE that interacts with the TOE.

Identity -- A representation (e.g., a string) uniquely identifying an Authorized Administrator, which can either be the full or abbreviated name of that administrator or a pseudonym.

Authentication data -- Information used to verify the claimed identity of an Authorized Administrator.

Peer TOEs -- Multiple, mutually authenticated TOEs that interact with each other. At a minimum, this includes a local (physically close) and a remote (physically distant) TOE.

Enclave – A collection of external IT entities that depend upon a TOE to provide VPN functions across a communications infrastructure.

VPN -- A Virtual Private Network (VPN) provides the ability to use a network (e.g., Internet, NIPRNET) as if it were a secure, private network.

1.5 RELATED PROTECTION PROFILES

18 The following PPs are related to this PP:

- *A Goal VPN Protection Profile for Protecting Sensitive Information*, Version 2.0 [3].
- *U.S. Government Traffic-Filter Firewall Protection Profile for Low Risk Environments* [4].
- *U.S. Department of Defense Application-level Firewall Protection Profile for Basic Robustness Environments* [5].

19 The Goal VPN PP provided a foundation for the development of this PP. The two firewall PPs were both created for use in low-risk, basic robustness environments and provide background source material for the development of this PP. The firewall PPs may also be used in conjunction with this PP to design secure networks.

1.6 PP ORGANIZATION

20 Section 1, PP Introduction, provides document management and overview information necessary to identify the PP along with references to other related PPs.

21 Section 2, Target of Evaluation (TOE) Description, defines the TOE and establishes the context of the TOE by referencing generalized security requirements.

22 Section 3, TOE Security Environment (TSE), describes the expected environment that the TOE is to be used. This section defines the set of threats that are relevant to the secure operation of the TOE, organizational security policies with which the TOE must comply, and secure usage assumptions applicable to this analysis.

23 Section 4, Security Objectives, defines the set of security objectives to be satisfied by the TOE and by the TOE operating environment.

24 Section 5, IT Security Requirements, defines the functional and assurance requirements derived from the Common Criteria, Part 2 and Part 3, respectively, that must be satisfied by the TOE.

25 Section 6, Rationale, provides rationale to demonstrate that the security objectives satisfy the threats and polices. This section also explains how the set of requirements are complete relative to the security objectives and presents a set of arguments that address dependency analysis and Strength of Function (SOF).

26 References are provided as background material for further investigation by interested users of the Protection Profile.

27 Expansion of acronyms are provided to facilitate comprehension of frequently used terms.

2 TARGET OF EVALUATION (TOE) DESCRIPTION

28 A VPN provides the ability to use a public network, such as the Internet, as if it were a secure, private network. A VPN is created through the use of devices that can establish secure communication channels over a common, untrusted (or less trusted) communications infrastructure, protecting data in-transit between two communicating entities.[1] The secure communications channels are established using security mechanisms such as encryption, digital signatures, identification and authentication, and access controls. Such secure communications channels may be established over Local Area Networks (LANs), Campus Area Networks (CANs), Metropolitan Area Networks (MANs), privately owned Wide Area Networks (WANs), or public WANs (e.g., the Internet).

29 The TOE is instantiated by a device at each enclave boundary. The TOE is a VPN functional component that may either be hosted on a firewall or router, or may be a dedicated VPN gateway device. Each TOE authenticates itself to its peer, agrees upon cryptographic keys and algorithms, securely generates and distributes session keys as necessary, and encrypts network traffic in accordance with the TOE security policy. The TOE will enforce the same security policy between communicating peers.

30 As shown in Figure 1 - VPN Architecture, a system in enclave "A" is able to communicate with a system in enclave "C" via a secure channel while simultaneously communicating with a system in enclave "B" without encryption or authentication of the communication stream. As a result, the TOE at enclave "A" is capable of creating VPN connections as well as non-VPN connections. This mechanism is known as a "VPN bypass capability." The use or non-use of a secure channel is dictated by the security policy configuration enforced by the TOE.

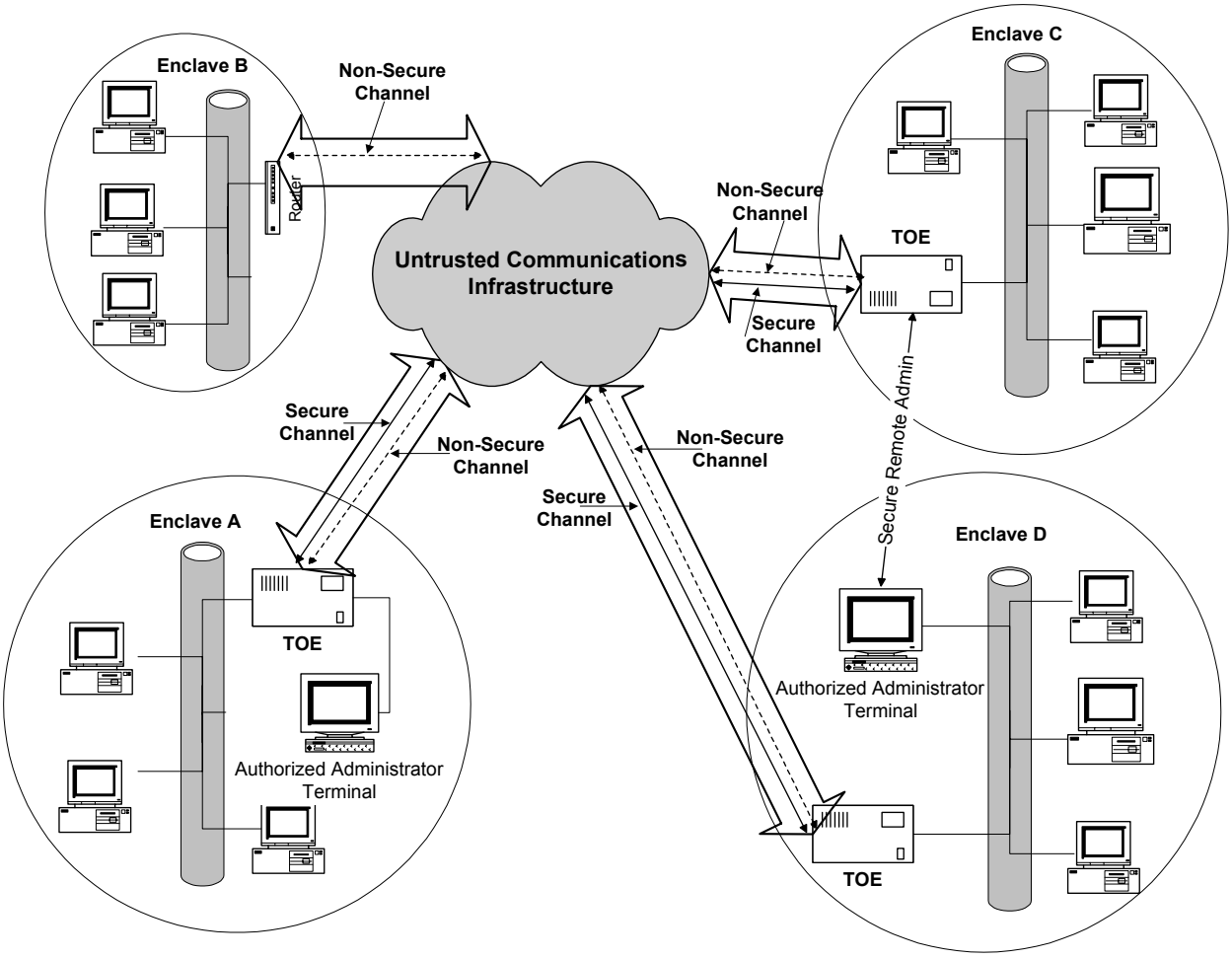
31 The TOE will enforce a security policy as follows:

- for outbound traffic associated with a peer TOE, the local TOE will create or use an existing secure channel between the peer TOEs;
- for outbound traffic not associated with a peer TOE, the local TOE will not invoke the security mechanisms and a secure channel will not be established;
- for inbound traffic associated with a peer TOE, the local TOE will create or use an existing secure channel between the peer TOEs; and
- for inbound network traffic not associated with a peer TOE, the local TOE will not invoke the security mechanisms and a secure channel will not be established.

32 The TOEs will exchange identities and will perform two types of authentication: device-level authentication of peer TOEs and user authentication of the Authorized

[1] This is often referred to as a *Secure VPN Tunnel*.

Administrator. Device-level authentication enables a TOE to construct a secure channel with a trusted peer. The secure channel should be established only after each device authenticates itself. Device-level authentication is performed by authentication technologies, such as digital signatures. The TOE will assure that the trust establishment is mutual. In other words, peers will mutually authenticate themselves to each other before establishing the secure channel.



33

Figure 1 - VPN Architecture

34 Users of the TOE consist of Authorized Administrators and external IT entities (e.g. PCs, workstations). External IT entities are not required to authenticate themselves to the TOE since they are only permitted to pass information through the TOE. Authorized Administrators must authenticate themselves to the TOE. Technologies used by the TOE to authenticate the Authorized Administrator to the TOE include, but are not limited to one-time-passwords, digital certificates, or biometrics. Authorized Administrators may administer the TOE locally (via a secure channel connection or a physically protected direct connection to a console port) or remotely (via a secure channel connection) as shown in Figure 1.

35 Audit events include modifications to the group of individuals associated with the Authorized Administrator role; use of the identification and authentication mechanisms (including any attempted reuse of authentication data); changes made to the TOE's security policy rules, mechanisms and data; actions taken due to imminent security violations; decisions made by the TOE to enforce security policy rules; changes to the TOE's date and time; and the use of other security functions. The decision to record auditable events will be made in accordance with organizational security policy and implemented by the Authorized Administrator. If the audit trail becomes full then the only auditable events that are recorded are those performed by the Authorized Administrator. Audit trail data is stamped with a dependable date and time when recorded.

36 The TOE shall implement VPN mechanisms using technologies such as cryptography, key management, access control, authentication, and data integrity. TOEs meeting this PP will implement and conform to the Internet Engineering Task Force (IETF) Internet Protocol Security (IPSEC) Encapsulating Security Payload (ESP) protocol as specified in RFC 2406. TOE encryption mechanisms will conform to IETF *ESP CBC-Mode Cipher Algorithms* as specified in RFC 2451. The TOE shall, at a minimum, implement the Triple DES (3DES) algorithm as specified in FIPS PUB 46-3 and with usage for ESP outlined in RFC 2451. TOE data integrity mechanisms will conform to IETF *Use of HMAC-SHA-1-96 within ESP and AH* as specified in RFC 2404. The TOE shall utilize cryptographic modules that are compliant with FIPS PUB 140-2. The TOE shall perform key management and key exchange using the IETF specified Internet Key Exchange (IKE) (RFC 2409) which shall be FIPS PUB 140-2 compliant.

37 The TOE shall, at a minimum, meet all of the assurance requirements defined by Part 3 of the CC for EAL2.

3 TOE SECURITY ENVIRONMENT

38 *Guidance and Policy for the Department of Defense Global Information Grid Information Assurance (GIG)* [2] requires that all information systems be assigned a mission category that reflects the type of information processed by the system. TOEs compliant with this PP will be capable of processing unclassified Mission Support or Administrative data over any network, or Mission Critical data (i.e., data that is vital to the operational readiness or mission effectiveness in terms of timeliness and content) over an encrypted network.[2]

39 The GIG also requires that all information systems employ protection mechanisms according to the level of robustness required relative to the sensitivity of the data to be protected and the threat agents likely to be involved. TOEs compliant with this PP are intended to be used in a Basic Robustness Environment (BRE). Basic Robustness is defined in the GIG policy as: "security features and assurances that equate to good commercial practice and includes NIST validated cryptography, EAL1 or greater assurance, Class 3 PKI certificates, and Authorized Administrator authentication."[3]

40 The remainder of this section addresses the following:

- Assumptions about the security aspects of a compliant TOE environment;
- Threats to TOE assets or to the TOE environment which must be countered; and
- Organizational security policies that compliant TOEs must enforce.

3.1 ASSUMPTIONS

41 The specific conditions below are assumed to exist in a PP-compliant TOE environment.

A.CRYPTANALYTIC

42 Cryptographic methods used in the TOE will be independently evaluated to be FIPS 140-2 compliant and will be shown to be resistant to cryptanalytic attacks (i.e., will be of adequate strength to protect unclassified mission support or administrative data).

A.HARDENED

43 The underlying operating system will be hardened to remove all mechanisms and services that are not required by the TOE.

---

[2] The encryption capabilities of the encrypted network are not provided by the TOE.

[3] This Protection Profile defines assurances that equate to EAL2, as defined in Part 3 of the CC.

A.NO_ENCLAVE_PROTECTION

44 The TOE will not protect the confidentiality or integrity of data from threat agents inside an enclave. However, the TOE will protect the confidentiality and integrity of data in transit between peer TOEs.

A.NO_EVIL

45 Authorized Administrators are non-hostile, appropriately trained and follow all administrator guidance. However, they are capable of error.

A.NO_GENERAL_PURPOSE

46 There are no general-purpose computing or storage repository capabilities (e.g., compilers, editors, or user applications) available on the TOE.

A.NO_PUBLIC_DATA

47 The TOE only hosts TOE data and therefore does not host public data.

A.PHYSICAL_SECURITY

48 The TOE will reside in a physically secure environment.

A.SECURITY_POLICY

49 Peer TOEs will be administered to enforce compatible[4] security policies.

A.TOE_ENTRY_POINT

50 Information cannot flow between external IT entities located in different enclaves without passing through the TOE.

3.2 THREATS

51 PPs are required to define threats that may be broadly categorized as threats to the TOE and threats to the operating environment. Threats to the TOE have been tailored based on the definition of a Basic Robustness Environment (BRE). In particular, threats associated with availability, TEMPEST, covert channels, and coding errors have been excluded from consideration. Attacks by sophisticated threat agents and improper use of the TOE bypass capability are also not considered. The threats to the TOE are as follows:

- Threats associated with replay, masquerading and address spoofing;
- Threats associated with the compromise or corruption of audit data;
- Threats regarding the compromise of cryptographic functions or keys;

[4] Compatible is defined to mean that a core set of policy rules are identical and any differences are more restrictive.

- Threats associated with the destruction of critical TOE configuration data; and
- Threats associated with the loss of confidentiality and integrity of TOE data.

3.2.1 THREATS ADDRESSED BY THE TOE

52 The threats discussed below are addressed by PP compliant TOEs. The threat agents are unauthorized persons or external IT entities not authorized to access the TOE (i.e., administer the TOE).

T.ADDRESS_SPOOFING

53 A threat agent may circumvent the TOE's security policy by spoofing the source address in order to masquerade as an Authorized Administrator or external IT entity.

T.ATTACK_CONFIGURATION_DATA

54 A threat agent may attempt to read, modify, or destroy security-critical TOE configuration data.

T.ATTACK_POTENTIAL

55 A threat agent, using obvious vulnerabilities, may attempt to bypass the TOE security functions to gain access to the TOE or the assets it protects.[5]

T.AUDIT_FULL

56 A threat agent may cause audit records to be lost or prevent future records from being recorded by taking actions to exhaust storage capacity, thus masking an attacker's actions.

T.AUDIT_UNDETECTED

57 A threat agent may cause auditable events to go undetected.

T.BRUTE_FORCE

58 A threat agent may repeatedly try to guess Authorized Administrator's authentication data in order to launch an attack against the TOE.

T.CRYPTOGRAPHIC_ATTACK

59 A threat agent, using a cryptographic attack, may obtain information for which they are not authorized.

---

[5] This PP specifies threats equal to levels T2 or T3 as defined in the Information Assurance Technical Framework (IATF) Robustness Strategy. T2 is defined as a passive adversary with minimal resources who is willing to take little risk. T3 is defined as an adversary with minimal resources who is willing to take significant risk.

T.KEY_COMPROMISE

60 A threat agent, through the use of stolen or compromised cryptographic keys, may decrypt sensitive data and gain unauthorized access to sensitive data.

T.MASQUERADE

61 A threat agent, through the use of stolen or compromised cryptographic keys, may masquerade as a peer TOE, thereby gaining unauthorized access to sensitive data. Additionally, a threat agent, through the use of captured identification and authentication data, may masquerade as an Authorized Administrator of the TOE.

T.REPLAY

62 A threat agent may replay valid identification and authentication information that has been changed to disguise itself as an Authorized Administrator of the TOE.

3.2.2 THREATS ADDRESSED BY THE OPERATING ENVIRONMENT

63 Threats to the operating environment are associated with misconfiguration of the TOE. These threats will be countered by procedural measures or administrative methods.

T.CONFIGURATION

64 The TOE may be inadvertently configured, administered or used in an insecure manner by an Authorized Administrator.

T.POOR_MAINTENANCE

65 Authorized Administrators may not install software or hardware patches correcting known problems that may result in a compromise of confidentiality or integrity of TOE data.

3.3 ORGANIZATIONAL SECURITY POLICIES

66 The organizational security policies described below are addressed by PP-compliant TOEs.

P.ACCOUNTABILITY

67 Authorized Administrators shall be held accountable for all security-relevant actions.

P.ADMINISTRATION

68 Authorized Administrators shall administer the TOE locally or remotely through protected communications channels.

P.AUDIT_REVIEW

69 Audit data shall be reviewed, analyzed, and acted upon, when necessary.

P.BYPASS

70 All network traffic not sent to a peer TOE shall be allowed to bypass the TOE security mechanisms. Specifically, for outbound traffic not associated with a peer TOE, the local TOE will not invoke the security mechanisms and a secure channel will not be established. Likewise, for inbound network traffic not associated with a peer TOE, the local TOE will not invoke the security mechanisms and a secure channel will not be established.

P.CONFIDENTIALITY

71 All network traffic sent to or received from addresses associated with a peer TOE shall be encrypted or decrypted by the TOE where specified by the security policy. Specifically, for outbound traffic associated with a peer TOE, the local TOE will create or use an existing secure channel between the peer TOEs. Likewise, for inbound traffic associated with a peer TOE, the local TOE will create or use an existing secure channel between the peer TOEs.

P.CRYPTO

72 The TOE shall support the IETF *Internet Protocol Security Encapsulating Security Payload* (IPSEC ESP) as specified in RFC 2406. The TOE shall utilize, at a minimum, the Triple DES (3DES) algorithm as specified in *ESP CBC-Mode Cipher Algorithms* (RFC 2451). The TOE shall utilize cryptographic modules that are compliant with FIPS PUB 140-2.

P.INTEGRITY

73 The TOE shall support the IETF *Internet Protocol Security Encapsulating Security Payload* (IPSEC ESP) as specified in RFC 2406. Sensitive information transmitted to a peer TOE shall apply integrity mechanisms as specified in *Use of HMAC-SHA-1-96 within ESP and AH* (RFC 2404).

P.KEY_MANAGEMENT

74 The TOE shall support the IETF Internet Key Exchange (IKE) for key management and key exchange as specified in RFC 2409.

4 SECURITY OBJECTIVES

75 This chapter describes the security objectives for the Target of Evaluation (TOE) and the operating environment. The security objectives are divided between TOE Security Objectives (i.e., security objectives addressed directly by the TOE) and Security Objectives for the Operating Environment (i.e., security objectives addressed by the IT domain or by non-technical or procedural means).

4.1 TOE SECURITY OBJECTIVES

76 This section defines the security objectives that are to be addressed by the TOE.

O.ACCOUNTABILITY

77 The TOE must provide accountability of peer TOEs and of Authorized Administrator use of security functions before granting access to TOE functions.

O.ADMINISTRATION

78 The TOE must provide administrative tools to enable Authorized Administrators to effectively manage and maintain the TOE. These tools must be available through remote access, direct connection, or locally to the Authorized Administrator.

O.AUDIT

79 The TOE must provide a means to accurately detect and record security-relevant events in audit records.

O.CONFIDENTIALITY

80 The TOE must protect the confidentiality of data[6] between peer TOEs via the use of encryption. Additionally, the TOE must protect the confidentiality of its dialogue with an Authorized Administrator, either locally or remotely, through encryption.

O.EVALUATION_ASSURANCE_LEVEL

81 The TOE must demonstrate that it meets all of the assurance requirements defined in EAL2 in Part 3 of the CC.

[6] The authors understand that not all data will be protected by confidentiality. This objective is concerned with the protection of "sensitive" data transmitted through the TOE. The authors definition of "sensitive" data and, consequently, the "data" referenced by this objective, is "payload" (versus metadata) data.

O.INTEGRITY

82 The TOE must protect the integrity of data transmitted to a peer TOE via encryption. Upon receipt of data from a peer TOE, the TOE must verify that the received data accurately represents the data that was originally transmitted.

O.MEDIATE

83 The TOE must mediate the flow of information between peer TOEs in accordance with its security policy.

O.SECURITY_INFRASTRUCTURE

84 The TOE must protect the confidentiality and integrity of key management data and must ensure the proper exchange of keys.

O.SELF_PROTECT

85 From its initial startup, the TOE must protect itself against attempts to modify, deactivate, or circumvent the TOE security functions.

4.2 SECURITY OBJECTIVES FOR THE OPERATING ENVIRONMENT

86 This section defines the security objectives that are to be addressed by the IT domain or by non-technical or procedural means. All of the assumptions stated in Section 3.1 are considered to be security objectives for the environment. There is an additional objective for the environment, OE.CONFIGURATION. The mapping and rationale for the security objectives are described in Section 6.

OE.CONFIGURATION

87 The TOE, and any underlying operating system and hardware, must be installed, administered, and maintained (i.e., security-related hardware and software fixes) in a manner that preserves the integrity and confidentiality of TOE data (e.g., configuration data, administrative data, etc.) and data traversing the TOE.

OE.CRYPTANALYTIC

88 Cryptographic methods used in the TOE will be independently evaluated to be FIPS 140-2 compliant and will be shown to be resistant to cryptanalytic attacks (i.e., will be of adequate strength to protect unclassified mission support or administrative data).

OE.HARDENED

89 The underlying operating system will be hardened to remove all mechanisms and services that are not required by the TOE.

OE.NO_ENCLAVE_PROTECTION

90 The TOE will not protect the confidentiality or integrity of data from threat agents inside an enclave. However, the TOE will protect the confidentiality and integrity of data in transit between peer TOEs.

OE.NO_EVIL

91 Authorized Administrators are non-hostile, appropriately trained and follow all administrator guidance. However, they are capable of error.

OE.NO_GENERAL_PURPOSE

92 There are no general-purpose computing or storage repository capabilities (e.g., compilers, editors) available on the TOE.

OE.NO_PUBLIC_DATA

93 The TOE only hosts TOE data and therefore does not host public data.

OE.PHYSICAL_SECURITY

94 The TOE will reside in a physically secure environment.

OE.SECURITY_POLICY

95 Peer TOEs will be administered to enforce compatible security policies.

OE.TOE_ENTRY_POINT

96 Information cannot flow between external IT entities on different enclaves without passing through the TOE.

5 IT SECURITY REQUIREMENTS

97 This section provides functional and assurance requirements that must be satisfied by a Protection Profile-compliant TOE. These requirements consist of functional components from Part 2 of the CC and an Evaluation Assurance Level (EAL) containing assurance components from Part 3 of the CC.

5.1 TOE FUNCTIONAL SECURITY REQUIREMENTS

98 The functional security requirements for the TOE consist of the following components derived from Part 2 of the CC, summarized in Table 5.1 below. The functional components are presented in alphabetical order by component name in the CC.

Functional Components	
FAU_ARP.1	Security Alarms
FAU_GEN.1	Audit Data Generation
FAU_SAA.1	Potential Violation Analysis
FAU_SAR.1	Audit Review
FAU_STG.1	Protected Audit Trail Storage
FAU_STG.3	Action in Case of Possible Audit Data Loss
FAU_STG.4	Prevention of Audit Data Loss
FCS_CKM.1	Cryptographic Key Generation
FCS_CKM.2	Cryptographic Key Distribution
FCS_CKM.4	Cryptographic Key Destruction
FCS_COP.1	Cryptographic Operation
FDP_DAU.1	Basic Data Authentication
FDP_IFC.1	Subset Information Flow Control
FDP_IFF.1	Simple Security Attributes
FIA_AFL.1	Authentication Failure Handling
FIA_ATD.1	User Attribute Definition
FIA_UAU.2	User Authentication Before Any Action
FIA_UAU.4	Single Use Authentication
FIA_UID.2	User Identification Before Any Action
FMT_MOF.1	Management of Security Functions Behavior
FMT_MSA.1	Management of Security Attributes
FMT_MSA.2	Secure Security Attributes

Functional Components	
FMT_MSA.3	Static Attribute Initialization
FMT_MTD.1[7]	Management of TSF Data
FMT_MTD.2	Management of TSF Limits on TSF Data
FMT_MTD.3	Secure TSF Data
FMT_SMR.1	Security Roles
FPT_AMT.1	Abstract Machine Testing
FPT_RPL.1	Replay Detection
FPT_RVM.1	Non-bypassability of the TSP
FPT_SEP.1	TSF Domain Separation
FPT_STM.1	Reliable Time Stamps
FPT_TST.1	TSF Testing

Table 5.1 - Security Functional Requirements

5.1.1 SECURITY AUDIT (FAU)

FAU_ARP.1 Security alarms

99 FAU_ARP.1.1 - The TSF shall take [action to detect audit events, alert the Authorized Administrator, generate and record audit records in the audit trail] upon detection of a potential security violation.

FAU_GEN.1 Audit data generation

100 FAU_GEN.1.1 - The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the *minimum* level of audit; and

c) [the events in Table 5.2].

[7] There are three iterations of the component FMT_MTD.1 included in the PP, but for brevity, only one is listed in the table.

101 FAU_GEN.1.2 - The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, **Authorized Administrator** identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [information specified in column three of Table 5.2].

Functional Component	Auditable Event	Additional Audit Record Contents
FAU_ARP.1	Actions taken due to imminent security violations.	The presumed address of the source and destination subject.
FAU_SAA.1	Enabling and disabling of the analysis mechanism.	The identity of the Authorized Administrator performing the operation.
FCS_CKM.1	Success and failure of the activity.	The presumed address of the source and destination subject.
FCS_CKM.2	Success and failure of the activity.	The presumed address of the source and destination subject.
FCS_CKM.4	Success and failure of the activity.	The presumed address of the source and destination subject.
FCS_COP.1	Success and failure and type of cryptographic operation.	The presumed address of the source and destination subject.
FDP_DAU.1	Successful generation of validity evidence.	The presumed address of the source and destination subject.
FDP_IFF.1	Decisions to permit information flows.	The presumed address of the source and destination subject.
FIA_AFL.1	Reaching the threshold of unsuccessful authentication attempts and actions taken, and restoration to normal operational state.	The identity of the offending user and the Authorized Administrator.
FIA_UAU.2	Unsuccessful use of authentication mechanisms.	The user identities presented to the TOE.
FIA_UAU.4	Attempts to reuse authentication data.	The user identities presented to the TOE.

Functional Component	Auditable Event	Additional Audit Record Contents
FIA_UID.2	Unsuccessful use of the user identification mechanism, including the user identity provided.	The user identities presented to the TOE.
FMT_MSA.2	All offered and rejected values for a security attribute.	The presumed address of the source and destination subject.
FMT_MTD.3	All rejected values of TOE data.	The presumed address of the source and destination subject.
FMT_SMR.1	Modifications to the group of users that are part of the Authorized Administrator role.	The identity of the Authorized Administrator performing the modification and the user identity being associated with the Authorized Administrator role.
FPT_STM.1	Changes to the time.	The identity of the Authorized Administrator performing the operation.

Table 5.2 - Auditable Events

102 Application Note: The TOE can make no claim regarding the validity of the address of any source or destination subject. The TOE can only suppose that these addresses are accurate. Therefore, a "presumed address" is used to identify source and destination addresses.

FAU_SAA.1 Potential violation analysis

103 FAU_SAA.1.1 – The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TSP.

104 FAU_SAA.1.2 – The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of [unsuccessful use of authentication mechanisms and cryptographic operation failure] known to indicate a potential security violation;

b) [other events {to be determined by the Security Target writer}].

FAU_SAR.1 Audit review

105 FAU_SAR.1.1 - The TSF shall provide [an Authorized Administrator] with the capability to read [all audit data] from the audit records.

106 FAU_SAR.1.2 - The TSF shall provide the audit records in a manner suitable for the **Authorized Administrator** to interpret the information.

FAU_STG.1 Protected audit trail storage

107 FAU_STG.1.1 - The TSF shall protect the stored audit records from unauthorized deletion.

108 FAU_STG.1.2 - The TSF shall be able to *prevent* modifications to the audit records.

FAU_STG.3 Action in case of possible audit data loss

109 FAU_STG.3.1 - The TSF shall take [measures to notify the Authorized Administrator] if the audit trail exceeds [90% storage capacity].

FAU_STG.4 Prevention of audit data loss

110 FAU_STG.4.1 - The TSF shall *prevent auditable events, except those taken by the authorized* ***administrator*** and [shall limit the number of audit records lost] if the audit trail is full.

111 Application Note: The Security Target writer(s) is expected to provide, as part of their "Security requirements rationale" section, an analysis of the maximum amount of audit data that can be expected to be lost in the event of audit storage failure, exhaustion, and/or attack.

5.1.2 CRYPTOGRAPHIC SUPPORT (FCS)

FCS_CKM.1 Cryptographic key generation

112 FCS_CKM.1.1 – **At a minimum,** the TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [Triple Data Encryption Standard (3DES) as specified in FIPS PUB 46-3 and implementing any mode of operation specified in FIPS PUB 46-3 with Keying Option 1 (K1, K2, K3 are independent keys)] and specified cryptographic key sizes [that are 192 binary digits in length] that meet the following: [FIPS PUB 46-3 with Keying Option 1 and FIPS PUB 140-2 (Level 1)].

FCS_CKM.2 Cryptographic key distribution

113 FCS_CKM.2.1 – The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [performed by commercially available Internet Key Exchange (IKE) implementations] that meets the following: [FIPS PUB 140-2 (Level 1) and ANSI X9-17].

FCS_CKM.4 Cryptographic key destruction

114 FCS_CKM.4.1 - The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [which zeroizes all plaintext cryptographic keys and other unprotected security parameters within the device] that meets the following: [FIPS PUB 140-2, Security Level 1].

FCS_COP.1 Cryptographic operation

115 FCS_COP.1.1 - The TSF shall perform [encryption, decryption, and secure hash of network traffic[8] as defined in the TOE security policy] in accordance with a specified cryptographic algorithm: [Triple Data Encryption Standard (3DES) as specified in RFC 2451 and implementing any mode of operation specified in FIPS PUB 46-3 with Keying Option 1 (K1, K2, K3 are independent keys)] and cryptographic key sizes [that are 192 binary digits in length] that meet the following: [FIPS PUB 46-3 with Keying Option 1 and FIPS PUB 140-2 (Level 1) and HMAC-SHA-1-96 within ESP and AH (RFC 2404)].

116 Application Note: Triple DES encryption must protect all communications over the secure channel (including between the Authorized Administrator and the TOE both remotely and locally), and the associated cryptographic module(s) must comply at a minimum with FIPS PUB 140-2 Level 1. A future migration to the Advanced Encryption Standard (AES) is anticipated when the national standards are established. The intent of this requirement is not for the evaluator to perform a FIPS PUB 140-2 evaluation; rather, the evaluator will check for a certificate, verifying that the module completed a FIPS PUB 140-2 evaluation.

5.1.3 USER DATA PROTECTION (FDP)

FDP_DAU.1 Basic data authentication

117 FDP_DAU.1.1 - The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of [data transmitted to and from the TOE].

118 FDP_DAU.1.2 - The TSF shall provide [the Authorized Administrator] with the ability to verify **unsuccessful generation of validity** evidence of the indicated information.

FDP_IFC.1 Subset information flow control

119 FDP_IFC.1.1 - The TSF shall enforce the [AUTHENTICATED SFP] on:

a) [subjects: external IT entities that send and receive information through the TOE to one another;

b) information: traffic sent through the TOE; and

[8] Network traffic also includes the remote and local sessions of Authorized Administrators.

c) operation: pass encrypted information based on destination IP address and pass unencrypted (i.e., plain text) information based on destination IP address].

FDP_IFF.1 Simple security attributes

120 FDP_IFF.1.1 - The TSF shall enforce the [AUTHENTICATED SFP] based on the following types of subject and information security attributes:

a) [Subject security attributes:

- presumed address; and
- other subject security attributes {to be determined by the Security Target writer(s)};

b) Information security attributes:

- presumed address of source subject;
- presumed address of destination subject; and
- other information security attributes {to be determined by the Security Target writer(s)}].

121 FDP_IFF.1.2 - The TSF shall permit an information flow between a controlled subject and another controlled object via a controlled operation if the following rules hold:

a) [Subjects on an internal network can cause information to be encrypted over a secure channel if:

- for outbound traffic associated with a peer TOE, the local TOE will create or use an existing secure channel between the peer TOEs; and
- for inbound traffic associated with a peer TOE, the local TOE will create or use an existing secure channel between the peer TOEs.

b) Subjects on a network can cause information to be sent unencrypted over an open channel if:

- for outbound traffic not associated with a peer TOE, the local TOE will not invoke the security mechanisms and a secure channel will not be established; and
- for inbound network traffic not associated with a peer TOE, the local TOE will not invoke the security mechanisms and a secure channel will not be established].

122 FDP_IFF.1.3 - The TSF shall enforce the [none].

123 FDP_IFF.1.4 - The TSF shall provide the following [none].

124 FDP_IFF.1.5 -The TSF shall explicitly authorize an information flow based on the following rules: [none].

125 FDP_IFF.1.6 - The TSF shall explicitly deny an information flow based on the following rules: [none].

5.1.4 IDENTIFICATION AND AUTHENTICATION (FIA)

126 TOE security functions implemented by a probabilistic or permutational mechanism (e.g., password or hash function) are required (at EAL2 and higher) to include a strength of function claim. Strength of Function shall be demonstrated for the single-use authentication mechanism by demonstrating compliance with the "Statistical random number generator tests" and the "Continuous random number generator test" found in section 4.9 of FIPS PUB 140-2 [7]. The single-use authentication mechanism must demonstrate SOF-basic, as defined in Part 1 of the CC.

FIA_AFL.1 Authentication failure handling

127 FIA_AFL.1.1 - The TSF shall detect when [a setable, non-zero number, {to be determined by the Security Target writer(s),}] **of** unsuccessful authentication attempts occur related to [Authorized Administrators attempting to authenticate locally or remotely].

128 FIA_AFL.1.2 - When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [prevent the offender from successfully authenticating itself to the TOE until an action is taken by the Authorized Administrator].

FIA_ATD.1 User attribute definition

129 FIA_ATD.1.1 - The TSF shall maintain the following list of security attributes belonging to an **Authorized Administrator**:

a) [identity;

b) association of human user with the Authorized Administrator role;

c) any other user security attributes {to be determined by the Security Target writer(s)}].

FIA_UAU.2 User authentication before any action

130 FIA_UAU.2.1 - The TSF shall require the **Authorized Administrator** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that **Authorized Administrator**.

FIA_UAU.4 Single-Use Authentication

131 FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to [one-time-passwords, digital certificates, or biometrics].

FIA_UID.2 User identification before any action

132 FIA_UID.2.1 - The TSF shall require each **Authorized Administrator** to identify itself before allowing any other TSF-mediated actions on behalf of that user.

5.1.5 SECURITY MANAGEMENT (FMT)

FMT_MOF.1 Management of security functions behavior

133 FMT_MOF.1.1 - The TSF shall restrict the ability to *enable, disable, determine and modify the behavior of* the functions:

- Security monitoring rules;
- Security alarm actions;
- Audit trail access;
- Actions for which replay is detected;
- Actions to be taken in case of imminent audit storage failure;
- Objects for which data authentication applies;
- Conditions under which abstract machine testing and self-test occurs; and
- Actions to be taken in the event of authentication failure

to [an Authorized Administrator].

FMT_MSA.1 Management of security attributes

134 FMT_MSA.1.1 - The TSF shall enforce the [AUTHENTICATED SFP] to restrict the ability to *modify, delete* or [create] the security attributes [information flow rules in FDP_IFF.1] to [an Authorized Administrator].

FMT_MSA.2 Secure security attributes

135 FMT_MSA.2.1 - The TSF shall ensure that only secure values are accepted for security attributes.

FMT_MSA.3 Static attribute initialization

136 FMT_MSA.3.1 - The TSF shall enforce the [AUTHENTICATED SFP] to provide *restrictive* default values for security attributes that are used to enforce the SFP.

137 FMT_MSA.3.2 - The TSF shall allow the [Authorized Administrator] to specify alternative initial values to override the default values when an object or information is created.

FMT_MTD.1 (1) Management of TSF data

138 FMT_MTD.1.1 - The TSF shall restrict the ability to *modify, delete* and [assign] the [authentication data in FIA_ATD.1] to [an Authorized Administrator].

FMT_MTD.1 (2) Management of TSF data

FMT_MTD.1.1 - The TSF shall restrict the ability to *modify* the [cryptographic key attributes in FCS_CKM.1] to [an Authorized Administrator].

FMT_MTD.1 (3) Management of TSF data

FMT_MTD.1.1 - The TSF shall restrict the ability to [set] the [time and date used to form the timestamps in FPT_STM.1] to [an Authorized Administrator].

FMT_MTD.2 Management of limits on TSF data

139 FMT_MTD.2.1 - The TSF shall restrict the specification of [the audit threshold, the time interval used for self-testing, the threshold for unsuccessful authentication attempts] to [an Authorized Administrator].

140 FMT_MTD.2.2 - The TSF shall take the following actions, if the TSF data are at, or exceed, the indicated limits: [actions specified in FAU_STG.3, FPT_TST.1 and FIA_AFL.1].

FMT_MTD.3 Secure TSF data

141 FMT_MTD.3.1 - The TSF shall ensure that only secure values are accepted for TSF data.

FMT_SMR.1 Security roles

142 FMT_SMR.1.1 - The TSF shall maintain the roles [Authorized Administrator].

143 FMT_SMR.1.2 - The TSF shall be able to associate users[9] with the **Authorized Administrator** role.

[9] The only "users" of the VPN are Authorized Administrators.

5.1.6 PROTECTION OF THE TOE SECURITY FUNCTIONS (FPT)

FPT_AMT.1 Abstract machine testing

144 FPT_AMT.1.1 – The TSF shall run a suite of tests *during initial start-up* to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.

FPT_RPL.1 Replay detection

145 FPT_RPL.1.1 - The TSF shall detect replay for the following entities: [peer TOE authentication and Authorized Administrator authentication].

146 FPT_RPL.1.2 - The TSF shall perform [ignore the attempted replay operation and generate an audit record] when replay is detected.

FPT_RVM.1 Non-bypassability of the TSP

147 FPT_RVM.1.1 - The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

FPT_SEP.1 TSF domain separation

148 FPT_SEP.1.1 - The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

149 FPT_SEP.1.2 - The TSF shall enforce separation between the security domains of subjects in the TSC.

FPT_STM.1 Reliable time stamps

150 FPT_STM.1.1 - The TSF shall be able to provide reliable time stamps for its own use.

FPT_TST.1 TSF testing

151 FPT_TST.1.1 - The TSF shall run a suite of self tests *during initial start-up, periodically during normal operation and at the request of the Authorized Administrator* to demonstrate the correct operation of the TSF.

152 FPT_TST.1.2 - The TSF shall provide **Authorized Administrators** with the capability to verify the integrity of TSF data.

153 FPT_TST.1.3 - The TSF shall provide **Authorized Administrators** with the capability to verify the integrity of stored TSF executable code.

5.2 TOE SECURITY ASSURANCE REQUIREMENTS

154 The assurance security requirements for this PP, taken from Part 3 of the CC, compose EAL2. These assurance components are summarized in the following table.

Assurance Class	Assurance Components	
Configuration management	ACM_CAP.2	Configuration items
Delivery and operation	ADO_DEL.1	Delivery procedures
	ADO_IGS.1	Installation, generation, and start-up procedures
Development	ADV_FSP.1	Informal functional specification
	ADV_HLD.1	Descriptive high-level design
	ADV_RCR.1	Informal correspondence demonstration
Guidance documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability assessment	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.1	Developer vulnerability analysis

Table 5.3 - Assurance Requirements: EAL2

ACM_CAP.2 Configuration items

Developer action elements:

155 ACM_CAP.2.1D - The developer shall provide a reference for the TOE.

156 ACM_CAP.2.2D - The developer shall use a CM system.

157 ACM_CAP.2.3D - The developer shall provide CM documentation.

Content and presentation of evidence elements:

158 ACM_CAP.2.1C - The reference for the TOE shall be unique to each version of the TOE.

159 ACM_CAP.2.2C - The TOE shall be labeled with its reference.

160 ACM_CAP.2.3C - The CM documentation shall include a configuration list.

161 ACM_CAP.2.4C - The configuration list shall describe the configuration items that comprise the TOE.

162 ACM_CAP.2.5C - The CM documentation shall describe the method used to uniquely identify the configuration items.

163 ACM_CAP.2.6C - The CM system shall uniquely identify all configuration items.

Evaluator action elements:

164 ACM_CAP.2.1E - The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_DEL.1 Delivery procedures

Developer action elements:

165 ADO_DEL.1.1D - The developer shall document procedures for delivery of the TOE or parts of it to the user.

166 ADO_DEL.1.2D - The developer shall use the delivery procedures.

Content and presentation of evidence elements:

167 ADO_DEL.1.1C - The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

Evaluator action elements:

168 ADO_DEL.1.1E - The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_IGS.1 Installation, generation, and start-up procedures

Developer action elements:

169 ADO_IGS.1.1D - The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

Content and presentation of evidence elements:

170 ADO_IGS.1.1C - The documentation shall describe the steps necessary for secure installation, generation, and start-up of the TOE. Evaluator action elements:

Evaluator action elements:

171 ADO_IGS.1.1E - The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

172 ADO_IGS.1.2E - The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

ADV_FSP.1 Informal functional specification

Developer action elements:

173 ADV_FSP.1.1D - The developer shall provide a functional specification.

Content and presentation of evidence elements:

174 ADV_FSP.1.1C - The functional specification shall describe the TSF and its external interfaces using an informal style.

175 ADV_FSP.1.2C - The functional specification shall be internally consistent.

176 ADV_FSP.1.3C - The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.

177 ADV_FSP.1.4C - The functional specification shall completely represent the TSF.

Evaluator action elements:

178 ADV_FSP.1.1E - The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

179 ADV_FSP.1.2E - The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

ADV_HLD.1 Descriptive high-level design

Developer action elements:

180 ADV_HLD.1.1D - The developer shall provide the high-level design of the TSF.

Content and presentation of evidence elements:

181 ADV_HLD.1.1C - The presentation of the high-level design shall be informal.

182 ADV_HLD.1.2C - The high-level design shall be internally consistent.

183 ADV_HLD.1.3C - The high-level design shall describe the structure of the TSF in terms of subsystems.

184 ADV_HLD.1.4C - The high-level design shall describe the security functionality provided by each subsystem of the TSF.

185 ADV_HLD.1.5C - The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

186 ADV_HLD.1.6C - The high-level design shall identify all interfaces to the subsystems of the TSF.

187 ADV_HLD.1.7C - The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

Evaluator action elements:

188 ADV_HLD.1.1E - The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

189 ADV_HLD.1.2E - The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

ADV_RCR.1 Informal correspondence demonstration

Developer action elements:

190 ADV_RCR.1.1D - The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

Content and presentation of evidence elements:

191 ADV_RCR.1.1C - For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

Evaluator action elements:

192 ADV_RCR.1.1E - The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_ADM.1 Administrator guidance

Developer action elements:

193 AGD_ADM.1.1D - The developer shall provide administrator guidance addressed to system administrative personnel.

194 Content and presentation of evidence elements:

195 AGD_ADM.1.1C - The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

196 AGD_ADM.1.2C - The administrator guidance shall describe how to administer the TOE in a secure manner.

197 AGD_ADM.1.3C - The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

198 AGD_ADM.1.4C - The administrator guidance shall describe all assumptions regarding user behavior that are relevant to secure operation of the TOE.

199 AGD_ADM.1.5C - The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

200 AGD_ADM.1.6C - The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

201 AGD_ADM.1.7C - The administrator guidance shall be consistent with all other documentation supplied for evaluation.

202 AGD_ADM.1.8C - The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

Evaluator action elements:

203 AGD_ADM.1.1E - The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_USR.1 User guidance

Developer action elements:

204 AGD_USR.1.1D - The developer shall provide user guidance.

Content and presentation of evidence elements:

205 AGD_USR.1.1C - The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

206 AGD_USR.1.2C - The user guidance shall describe the use of user-accessible security functions provided by the TOE.

207 AGD_USR.1.3C - The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

208 AGD_USR.1.4C - The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behavior found in the statement of TOE security environment.

209 AGD_USR.1.5C - The user guidance shall be consistent with all other documentation supplied for evaluation.

210 AGD_USR.1.6C - The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

Evaluator action elements:

211 AGD_USR.1.1E - The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_COV.1 Evidence of coverage

Developer action elements:

212 ATE_COV.1.1D - The developer shall provide evidence of the test coverage.

Content and presentation of evidence elements:

213 ATE_COV.1.1C - The evidence of the test coverage shall show the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

Evaluator action elements:

214 ATE_COV.1.1E - The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_FUN.1 Functional testing

Developer action elements:

215 ATE_FUN.1.1D - The developer shall test the TSF and document the results.

216 ATE_FUN.1.2D - The developer shall provide test documentation.

Content and presentation of evidence elements:

217 ATE_FUN.1.1C - The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.

218 ATE_FUN.1.2C - The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

219 ATE_FUN.1.3C - The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

220 ATE_FUN.1.4C - The expected test results shall show the anticipated outputs from a successful execution of the tests.

221 ATE_FUN.1.5C - The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

Evaluator action elements:

222 ATE_FUN.1.1E - The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2 Independent testing - sample

Developer action elements:

223 ATE_IND.2.1D - The developer shall provide the TOE for testing.

Content and presentation of evidence elements:

224 ATE_IND.2.1C - The TOE shall be suitable for testing.

225 ATE_IND.2.2C - The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

Evaluator action elements:

226 ATE_IND.2.1E - The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

227 ATE_IND.2.2E - The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

228 ATE_IND.2.3E - The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

AVA_SOF.1 Strength of TOE security function evaluation

Developer action elements:

229 AVA_SOF.1.1D - The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

Content and presentation of evidence elements:

230 AVA_SOF.1.1C - For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.

231 AVA_SOF.1.2C - For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

Evaluator action elements:

232 AVA_SOF.1.1E - The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

233 AVA_SOF.1.2E - The evaluator shall confirm that the strength claims are correct.

AVA_VLA.1 Developer vulnerability analysis

Developer action elements:

234 AVA_VLA.1.1D - The developer shall perform and document an analysis of the TOE deliverables searching for obvious ways in which a user can violate the TSP.

235 AVA_VLA.1.2D - The developer shall document the disposition of obvious vulnerabilities.

Content and presentation of evidence elements:

236 AVA_VLA.1.1C - The documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

Evaluator action elements:

237 AVA_VLA.1.1E - The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

238 AVA_VLA.1.2E - The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

6 RATIONALE

239 This chapter describes the rationale for the Security Objectives defined in Section 4 and the Security Requirements in Section 5. Additionally, this section describes the rationale for not satisfying all of the dependencies. Table 6.1 illustrates the mapping from Security Objectives to Threats and Policies.

6.1 RATIONALE FOR TOE SECURITY OBJECTIVES

O.ACCOUNTABILITY

240 This security objective is necessary to counter the threats and policy: T.ADDRESS_SPOOFING, T.BRUTE_FORCE, T.MASQUERADE, T.REPLAY, and P.ACCOUNTABILITY because it ensures that the Authorized Administrator is accountable for all security-relevant actions and peer TOEs are properly identified and authenticated.

O.ADMINISTRATION

241 This security objective is necessary to counter the threats and policy: T.ADDRESS_SPOOFING, T.BRUTE_FORCE, T.MASQUERADE, and P.ADMINISTRATION because it ensures that only Authorized Administrators can access administrative functions at all times and consequently can administer the TOE effectively.

O.AUDIT

242 This security objective is necessary to counter the threats: T.AUDIT_FULL and T.AUDIT_UNDETECTED because it ensures that security-relevant events are completely and accurately recorded.

O.CONFIDENTIALITY

243 This security objective is necessary to counter the threats and policies: T.CRYPTOGRAPHIC_ATTACK, T.KEY_COMPROMISE, P.CONFIDENTIALITY, and P.CRYPTO because it ensures that the TOE utilizes encryption and employs cryptography of adequate strength to protect sensitive data.

O.EVALUATION_ASSURANCE_LEVEL

244 This security objective is necessary to counter the threat and policy: T.ATTACK_POTENTIAL and P.BYPASS because it ensures that the TOE is resistant to penetration attacks performed by threat agents possessing minimal attack potential. Additionally, this security objective is necessary to ensure that the TOE enforces the security policy correctly.

O.INTEGRITY

245 This security objective is necessary to counter the threats and policies: T.ATTACK_CONFIGURATION_DATA, T.KEY_COMPROMISE, P.INTEGRITY, and P.KEY_MANAGEMENT because it ensures the integrity of TOE security-relevant data and keys.

O.MEDIATE

246 This security objective is necessary to counter the threats and policies: T.ADDRESS_SPOOFING, T.ATTACK_POTENTIAL, and P.BYPASS because it ensures that all information flowing between peer TOEs will be mediated in accordance with the TOE security policy.

O.SECURITY_INFRASTRUCTURE

247 This security objective is necessary to counter the threats and policies: T.ATTACK_CONFIGURATION_DATA, T.KEY_COMPROMISE, T.MASQUERADE, P.CONFIDENTIALITY, P.INTEGRITY, and P.KEY_MANAGEMENT because it ensures that the confidentiality and integrity of key management data and proper exchange of keys.

O.SELF_PROTECT

248 This security objective is necessary to counter the threats and policies: T.ATTACK_CONFIGURATION_DATA, T.ATTACK_POTENTIAL, and P.BYPASS because it ensures that the TOE is always invoked, tamperproof and not capable of being circumnavigated.

	O.ACCOUNTABILITY	O.ADMINISTRATION	O.AUDIT	O.CONFIDENTIALITY	O.EVALUATION_ASSURANCE_LEVEL	O.INTEGRITY	O.MEDIATE	O.SECURITY_INFRASTRUCTURE	O.SELF_PROTECT
T.ADDRESS_SPOOFING	X	X					X		
T.ATTACK_CONFIGURATION_DATA						X		X	X
T.ATTACK_POTENTIAL					X		X		X
T.AUDIT_FULL			X						
T.AUDIT_UNDETECTED			X						
T.BRUTE_FORCE	X	X							
T.CRYPTOGRAPHIC_ATTACK				X					
T.KEY_COMPROMISE				X		X		X	
T.MASQUERADE	X	X						X	
T.REPLAY	X								
P.ACCOUNTABILITY	X								
P.ADMINISTRATION		X							
P.BYPASS					X		X		X
P.CONFIDENTIALITY				X				X	
P.CRYPTO				X					
P.INTEGRITY						X		X	
P.KEY_MANAGEMENT						X		X	

Table 6.1 - Security Objectives to Threats/Policies Mapping

6.2 RATIONALE FOR SECURITY OBJECTIVES FOR THE ENVIRONMENT

249 All but one of the security objectives for the environment, OE.CONFIGURATION, is a restatement of an assumption found in Section 3. Therefore, those security objectives for the environment trace to the assumptions trivially. The non-IT security objective OE.CONFIGURATION is necessitated by the threats T.CONFIGURATION and T.POOR_MAINTENANCE and are addressed by the policies P.ADMINISTRATION, P.BYPASS and P.AUDIT_REVIEW. This additional non-IT security objective ensures that the TOE is properly administered.

6.3 RATIONALE FOR SECURITY REQUIREMENTS

250 The functional and assurance requirements presented in this PP are mutually supportive and their combination meets the stated security objectives. The security requirements were derived according to the general model presented in Part 1 of the Common Criteria. Table 6.1 demonstrates the relationship between the threat, policies and the TOE security objectives. Table 6.2 demonstrates the mapping between the security requirements and the security objectives. Together these tables demonstrate the completeness and sufficiency of the security requirements.

FAU_ARP.1 Audit Alarms

251 This component aids in the detection of intrusions and provides a function to alert the Authorized Administrator. This component traces back to and aids in meeting the following objectives: O.ADMINISTRATION and O.AUDIT.

FAU_GEN.1 Audit Data Generation

252 This component outlines the data that must be included in audit records and the events that must be audited. This component traces back to and aids in meeting the following objective: O.AUDIT.

FAU_SAA.1 Potential Violation Analysis

253 This component ensures that repeated failed attempts to authenticate or to encrypt data are monitored and alarmed if a threshold is reached. This component traces back to and aids in meeting the following objectives: O.AUDIT and O.SELF_PROTECT.

FAU_SAR.1 Audit Review

254 This component ensures that the audit is understandable by an Authorized Administrator. This component traces back to and aids in meeting the following objective: O.ADMINISTRATION.

FAU_STG.1 Protected Audit Trail Storage

255 This component ensures that the audit trail is always protected from tampering. Only the Authorized Administrator is permitted to access the audit trail. This component traces back to and aids in meeting the following objectives: O.ADMINISTRATION, O.INTEGRITY, and O.SELF_PROTECT.

FAU_STG.3 Action in Case of Possible Audit Data Loss

256 This component ensures that the Authorized Administrator is notified when the audit trail is reaching its maximum capacity. This component traces back to and aids in meeting the following objective: O.SELF_PROTECT.

FAU_STG.4 Prevention of Audit Data Loss

257 This component ensures that the Authorized Administrator will be able to administer the audit trail should it become full. This component also ensures that the actions taken by the Authorized Administrator will be recorded. This component traces back to and aids in meeting the following objectives: O.ADMINISTRATION and O.AUDIT.

FCS_CKM.1 Cryptographic Key Generation

258 This component ensures that the keys and key management data generated are of adequate strength to protect the confidentiality and integrity of data transmitted between peer TOEs. This component traces back to and aids in meeting the following objectives: O.CONFIDENTIALITY, O.INTEGRITY, and O.SECURITY_INFRASTRUCTURE.

FCS_CKM.2 Cryptographic Key Distribution

259 This component ensures that the keys and key management data are distributed securely to provide confidentiality and integrity of data transmitted between peer TOEs. This component traces back to and aids in meeting the following objectives: O.CONFIDENTIALITY, O.INTEGRITY, and O.SECURITY_INFRASTRUCTURE.

FCS_CKM.4 Cryptographic Key Destruction

260 This component ensures that the keys and key management data are correctly destroyed to protect the confidentiality and integrity of data transmitted between peer TOEs. This component traces back to and aids in meeting the following objectives: O.CONFIDENTIALITY, O.INTEGRITY, and O.SECURITY_INFRASTRUCTURE.

FCS_COP.1 Cryptographic Operation

261 This component ensures that all data sent between peer TOEs, including Authorized Administrator remote and local communications, are encrypted using Triple Data Encryption Standard (3DES). This component traces back to and aids in meeting the following objectives: O.CONFIDENTIALITY and O.INTEGRITY.

FDP_DAU.1 Basic Data Authentication

262 This component is needed to guarantee the validity of data sent between peer TOEs. It also ensures that the Authorized Administrator has the capability to verify the validity of the data. This component traces back to and aids in meeting the following objectives: O.ADMINISTRATION and O.INTEGRITY.

FDP_IFC.1 Subset Information Flow Control

263 This component identifies the entities involved in the AUTHENTICATED information flow control SFP. This component traces back to and aids in meeting the following objective: O.MEDIATE.

FDP_IFF.1 Simple Security Attributes

264 This component identifies the attributes of the subjects sending and receiving the information in the AUTHENTICATED SFP, as well as the attributes for the information itself. Then the operations identify under what conditions information is permitted to flow through the TOE. This component traces back to and aids in meeting the following objectives: O.MEDIATE.

FIA_AFL.1 Authentication Failure Handling

265 This component ensures that human users who are not Authorized Administrators cannot endlessly attempt to authenticate. After some number of failures, defined by the Authorized Administrator, the user is unable from that point on to authenticate. This component traces back to and aids in meeting the following objectives: O.ADMINISTRATION and O.SELF_PROTECT.

FIA_ATD.1 User Attribute Definition

266 This component exists to provide attributes to distinguish Authorized Administrators from one another for accountability purposes and to associate the role in FMT_SMR.1 with a user. This component traces back to and aids in meeting the following objective: O.ACCOUNTABILITY.

FIA_UAU.2 User Authentication Before Any Action

267 This component ensures that the Authorized Administrator is authenticated before any action is allowed by the TSF. This component traces back to and aids in meeting the following objective: O.ACCOUNTABILITY.

FIA_UAU.4 Single-Use Authentication

268 The component was chosen to ensure that Authorized Administrators use an authentication mechanism of adequate strength when authenticating to the TOE. This component traces back to and aids in meeting the following objective: O.ACCOUNTABILITY.

FIA_UID.2 User Identification Before Any Action

269 This component ensures that the Authorized Administrator identity is identified to the TOE before anything occurs on behalf of the Authorized Administrator. This component traces back to and aids in meeting the following objective: O.ACCOUNTABILITY.

FMT_MOF.1 Management of Security Functions Behavior

270 This component ensures that the TSF restricts the ability to modify the behavior of functions (e.g., audit trail management, replay detection, self-test, authentication failure) to an Authorized Administrator. This component traces back to and aids in meeting the following objective: O.ADMINISTRATION.

FMT_MSA.1 Management of Security Attributes

271 This component ensures that the TSF restricts the ability to add, delete, and modify the security attributes that affect the AUTHENTICATED SFP to only the Authorized Administrator. This component traces back to and aids in meeting the following objectives: O.ADMINISTRATION and O.MEDIATE.

FMT_MSA.2 Secure Security Attributes

272 This component ensures that appropriate values are assigned to the security attributes used in the AUTHENTICATED SFP. This component traces back to and aids in meeting the following objectives: O.SELF_PROTECT.

FMT_MSA.3 Static Attribute Initialization

273 This component ensures that there are restrictive default values implemented in the AUTHENTICATED SFP which the Authorized Administrator can change. This component traces back to and aids in meeting the following objectives: O.ADMINISTRATION and O.MEDIATE.

FMT_MTD.1 (1) Management of TSF Data

274 This component ensures that the TSF restricts the ability to modify, delete, and assign user attributes (as defined in FIA_ATD.1.1) to only the Authorized Administrator. This component traces back to and aids in meeting the following objective: O.ADMINISTRATION.

FMT_MTD.1 (2) Management of TSF Data

275 This component ensures that the TSF restricts the ability to modify the cryptographic key attributes (as defined in FCS_CKM.1) to only the Authorized Administrator. This component traces back to and aids in meeting the following objective: O.ADMINISTRATION.

FMT_MTD.1 (3) Management of TSF Data

276 This component ensures that the TSF restricts the ability to set the time and date used to form timestamps (as defined in FPT_STM.1) to only the Authorized Administrator. This component traces back to and aids in meeting the following objective: O.ADMINISTRATION.

FMT_MTD.2 Management of TSF Limits on TSF Data

277 This component ensures that the TSF restricts the specification of the number of authentication failures, the audit threshold, and the time interval for self-testing to the Authorized Administrator. This component traces back to and aids in meeting the following objective: O.ADMINISTRATION.

FMT_MTD.3 Secure TSF Data

278 This component was chosen to ensure that appropriate values are assigned to TSF data. This component traces back to and aids in meeting the following objectives: O.SELF_PROTECT.

FMT_SMR.1 Security Roles

279 This component was chosen because each of the FMT components depends on the assignment of a user to the Authorized Administrator role. This component traces back to and aids in meeting the following objective: O.ADMINISTRATION.

FPT_AMT.1 Abstract Machine Testing

280 This component ensures that the security assumptions provided by the underlying abstract machine are tested during start-up. This component traces back to and aids in meeting the following objective: O.SELF_PROTECT.

FPT_RPL.1 Replay Detection

281 This component ensures that replay of authentication attempts are detected and audited. This component traces back to and aids in meeting the following objectives: O.AUDIT and O.ACCOUNTABILITY.

FPT_RVM.1 Non-bypassability of the TSP

282 This component ensures that the TSF enforcement functions are always invoked from initial start-up. This component traces back to and aids in meeting the following objective: O.SELF_PROTECT.

FPT_SEP.1 TSF Domain Separation

283 This component ensures that the TSF has a domain of execution that is separate and that cannot be violated by unauthorized users. This component traces back to and aids in meeting the following objective: O.SELF_PROTECT.

FPT_STM.1 Reliable Time Stamps

284 This component was included because FAU_GEN.1 depends on having the date and time accurately recorded in the audit records. This component traces back to and aids in meeting the following objective: O.AUDIT.

FPT_TST.1 TSF Testing

285 This component ensures the integrity of the operation of the TSF and to provide the Authorized Administrator a means to verify the integrity of the TSF code and data. This component traces back to and aids in meeting the following objective: O.ADMINISTRATION and O.SELF_PROTECT. A summary of the security requirements to security objectives mapping is contained in the Table 6.2 below.

	O.ACCOUNTABILITY	**O.ADMINISTRATION**	**O.AUDIT**	**O.CONFIDENTIALITY**	**O.INTEGRITY**	**O.MEDIATE**	**O.SECURITY_ INFRASTRUCTURE**	**O.SELF_PROTECT**
FAU_ARP.1		X	X					
FAU_GEN.1			X					
FAU_SAA.1			X					X
FAU_SAR.1		X						
FAU_STG.1		X			X			X
FAU_STG.3								X
FAU_STG.4		X	X					
FCS_CKM.1				X	X		X	
FCS_CKM.2				X	X		X	
FCS_CKM.4				X	X		X	
FCS_COP.1				X	X			
FDP_DAU.1		X			X			
FDP_IFC.1						X		
FDP_IFF.1						X		
FIA_AFL.1		X						X
FIA_ATD.1	X							
FIA_UAU.2	X							
FIA_UAU.4	X							

	O.ACCOUNTABILITY	O.ADMINISTRATION	O.AUDIT	O.CONFIDENTIALITY	O.INTEGRITY	O.MEDIATE	O.SECURITY_INFRASTRUCTURE	O.SELF_PROTECT
FIA_UID.2	X							
FMT_MOF.1		X						
FMT_MSA.1		X				X		
FMT_MSA.2								X
FMT_MSA.3		X				X		
FMT_MTD.1		X						
FMT_MTD.1(2)		X						
FMT_MTD.1(3)		X						
FMT_MTD.2		X						
FMT_MTD.3								X
FMT_SMR.1		X						
FPT_AMT.1								X
FPT_RPL.1	X		X					
FPT_RVM.1								X
FPT_SEP.1								X
FPT_STM.1			X					
FPT_TST.1		X						X

Table 6.2 – Functional Requirements to Security Objectives Mapping

6.4 RATIONALE FOR ASSURANCE REQUIREMENTS

286 The EAL2 assurance level was chosen based on three factors:

- detailed conversations with the sponsor of the PP;
- recommendations documented in the GIG; and
- the postulated threat environment.

287 First and foremost, the PP sponsor did not wish to impose additional requirements on TOE developers. The EAL definitions in Part 3 of the CC were reviewed and EAL2 was believed to best achieve this goal. Specifically, Part 3 of the CC states that at EAL2, minimal additional tasks are imposed upon the vendor to the extent that if the vendor applies reasonable standards of care to the development, evaluation may be feasible without vendor involvement other than support for functional testing, strength of function analysis and vulnerability testing verification. The sponsor concluded that EAL2 equates to good commercial practice and should not require a substantial investment of cost or time on the part of the developer.

288 The Government's guidance in the GIG was consulted and found to also support the chosen assurance level. Specifically, the GIG states that good commercial practice equates to basic robustness environments, which by definition includes EAL2.

289 The postulated threat environment specified in Section 3 of the PP was used in conjunction with the Information Assurance Technical Framework (IATF) Robustness Strategy guidance to derive the chosen assurance level. In particular, the threat T.ATTACK_POTENTIAL implies that the TOE will be able to withstand attacks through obvious vulnerabilities. This threat specification equates to T2 or T3 as defined in the IATF Robustness Strategy. The degree of robustness definition includes an assurance level of EAL2.

290 These three factors were taken into consideration and the conclusion was that EAL2 was the appropriate level of assurance.

6.5 RATIONALE FOR NOT SATISFYING ALL DEPENDENCIES

291 With the exception of FMT_MSA.2 and FMT_MTD.3, all dependencies are contained in this Protection Profile. Both of these components have the assurance component ADV_SPM.1, Informal TOE Security Policy Model, as a dependency. The sponsor of the PP did not include ADV_SPM.1 because it was felt that the testing requirement specified in this PP would provide adequate assurance for a Basic Robustness Environment. ADV_SPM.1 is an EAL4 requirement and therefore is not aligned with the rationale provided for the chosen EAL.

6.6 RATIONALE FOR STRENGTH OF FUNCTION CLAIM

292 Part 1 of the CC defines "strength of function" in terms of the minimum efforts assumed necessary to defeat the expected security behavior of a TOE security function. There are three strength of function levels defined in Part 1, SOF-basic, SOF-medium and SOF-high. SOF-basic is the strength of function level chosen for this PP. SOF-basic states, "a level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential". The rationale for choosing SOF-basic was based on the TOE security objectives documented in Section 4 of this PP. In particular, the sponsor determined that the SOF-basic level is necessary and sufficient to address the TOE security objectives that counter the threat T.ATTACK_POTENTIAL. Consequently, the metrics (i.e., passwords and keys) chosen for inclusion in this Protection Profile were determined to be acceptable for SOF-basic and would adequately protect information in a Basic Robustness Environment.

REFERENCES

[1] *Common Criteria for Information Technology Security Evaluation,* CCIB-98-031 Version 2.1, August 1999.

[2] Department of Defense Chief Information Officer Guidance and Policy Memorandum No.6-8510, *Guidance and Policy for the Department of Defense Global Information Grid Information Assurance (GIG),* June 2000.

[3] *A Goal VPN Protection Profile for Protecting Sensitive Information,* Release 2.0, July 2000.

[4] *U.S. Government Traffic-Filter Firewall Protection Profile for Low Risk Environments*, April 1999.

[5] *U.S. Department of Defense Application-Level Firewall Protection Profile for Basic Robustness Environments,* June 2000.

[6] Federal Information Processing Standard Publication (FIPS-PUB) 46-3, *Data Encryption Standard (DES),* October 1999.

[7] Federal Information Processing Standard Publication (FIPS-PUB) 140-2, *Security Requirements for Cryptographic Modules,* May 25, 2001.

[8] *Implementing Virtual Private Networks,* Steven Brown, McGraw Hill, 1999.

[9] Internet Engineering Task Force, *IP Encapsulating Security Payload (ESP),* RFC 2406, November 1998.

[10] Internet Engineering Task Force, *Internet Key Exchange (IKE),* RFC 2409, November 1998.

[11] *Information Assurance Technical Framework,* Release 3.0, September 2000.

[12] Internet Engineering Task Force, *ESP CBC-Mode Cipher Algorithms,* RFC 2451, November 1998.

[13] Internet Engineering Task Force, *Use of HMAC-SHA-1-96 within ESP and AH,* RFC 2404, November 1998.

ACRONYMS

The following abbreviations from the Common Criteria are used in this Protection Profile:

AES	Advanced Encryption Standard
BRE	Basic Robustness Environment
CAN	Campus Area Network
CC	Common Criteria for Information Technology Security Evaluation
DES	Data Encryption Standard
DOD	Department of Defense
EAL	Evaluation Assurance Level
EBST&S	Enclave Boundary Security Technologies and Solutions
FIPS PUB	Federal Information Processing Standard Publication
GIG	Global Information Grid
IATF	Information Assurance Technical Framework
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IPSEC ESP	Internet Protocol Security Encapsulating Security Payload
IT	Information Technology
LAN	Local Area Network
MAN	Metropolitan Area Network
NSA	National Security Agency
PP	Protection Profile
SFP	Security Function Policy
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
TSP	TOE Security Policy
VPN	Virtual Private Network
WAN	Wide Area Network